A WHITE PAPER, PUBLIC DECLARATION, AND PRIOR ART PUBLICATION

THE HUMAN SOVEREIGNTY TECHNOLOGY PARADIGM

Technology Must Serve the Human. Never the Possessor.

Version 2.0 — Final Edition Including Voter Privacy, Second Amendment, and All Constitutional Provisions

PUBLICATION DATE	March 29, 2026
INVENTOR	Braydon Alexander Kershner
PATENT STATUS	US Provisional Patent Application Filed — PATENT PENDING
APPLICATION NO.	64/020,809
PATENT TITLE	Human Sovereignty Technology Platform: A Universal Operator-Bound Data Sovereignty, Emergency Sanitization, and Identity Authentication System
PURPOSE	Prevent government classification; Establish prior art on principles; Protect public domain; Prevent patent on tyrannical uses
ARCHIVES	Zenodo.org — Primary (CERN permanent DOI) | Internet Archive — archive.org/upload | arXiv.org — cs.CR category
LICENSE	CC0 1.0 Universal — Irrevocable Public Domain Dedication
CLASSIFICATION	Cannot be classified — constitutes published prior art at moment of filing per 35 U.S.C. § 102

LEGAL NOTICE: This document is published irrevocably in the public domain simultaneously with a provisional patent application. The principles, prohibitions, and application concepts described herein constitute prior art under 35 U.S.C. § 102 and equivalent international provisions as of the publication date. Classification under 35 U.S.C. § 181 or any equivalent statute of any jurisdiction is legally ineffective as to published material. Copies have been simultaneously deposited in multiple international archives and with multiple civil liberties organizations, ensuring permanent public availability regardless of any governmental action.

PREAMBLE: WHY THIS DOCUMENT MUST EXIST

This document is published on the same day as the filing of a provisional patent application for the Human Sovereignty Technology Platform. We publish it first — before any commercial announcement, any investor disclosure, any press release, any government briefing — for a single overriding reason: to ensure that the principles described herein are permanently in the public record before any government can prevent it.

The technology described in the accompanying patent is powerful. In the right hands, with the right design and the right implementation, it is one of the most significant tools for individual freedom ever conceived. In the wrong hands, or with the wrong implementation, it could become one of the most comprehensive instruments of control ever built. The difference between these two outcomes is not the technology itself. It is the principles governing its use.

By publishing these principles as prior art simultaneously with the patent filing, we accomplish three things. First, we prevent any government from classifying the principles as secret — published prior art cannot be retroactively classified. Second, we prevent any party from patenting the tyrannical uses of this technology — by publishing those uses as prior art, we dedicate them to the public domain and prevent anyone from owning the rights to surveillance, control, or oppression built on this platform. Third, we create a permanent, irrevocable, publicly-accessible record of what this technology is designed for and what it is expressly designed against.

> *A government powerful enough to classify an idea has already failed its people. The cure is not to fight classification after the fact. It is to publish before it can happen.*

PART I: THE PARADIGM SHIFT — FROM POSSESSION TO PERSONHOOD

The Failure of Possession-Based Technology

Every security system in existence today is built on a flawed premise: technology serves whoever possesses it. A seized laptop serves the seizing party. A captured credential serves the captor. A cloned key serves the thief. This creates an irresolvable vulnerability — the moment physical control of technology or credentials is lost, security fails. For individuals operating under high-threat conditions, this is not a theoretical concern. It is an operational reality that ends careers, destroys sources, and in some circumstances ends lives.

The technology described in the accompanying patent inverts this paradigm. Under the Operator-Bound Technology Principle, no technology functions for anyone other than its authenticated living operator. Seized equipment yields nothing. Captured credentials are worthless. Stolen devices are inert. The living physiology of the operator is the only key — and that key cannot be seized, copied, or replayed by any adversary.

The Operator-Bound Technology Principle

Technology is bound to the human operator who uses it. It functions exclusively for that living, authenticated operator. All data associated with operator sessions is stored exclusively in volatile form and purged completely when sessions end. Upon any defined threat condition, any selected portion of data, credentials, and system access is rendered permanently and forensically irrecoverable. Operational authority transfers to designated successors upon operator death without exposing the predecessor's credentials to adversaries.

This principle is not a product feature. It is a philosophy of technology design. Applied consistently across all technology — devices, vehicles, weapons, terminals, access systems, financial systems, electoral systems, medical systems, and all future technology — it creates a world in which technology cannot be turned against the person it serves.

PART II: THE THIRTEEN PRINCIPLES — PUBLIC DOMAIN

The following thirteen principles are irrevocably dedicated to the public domain under CC0 1.0. They may be used, cited, implemented, and built upon by any person, organization, government, or future generation without license or restriction. The tyrannical uses identified in Part III are also placed in the public domain — not to enable them but to prevent anyone from patenting them.

PRINCIPLE 1: OPERATOR PRIMACY

All technology exists to serve its authenticated human operator. No other party has authority over technology, data, or connected systems bound to an operator's identity without that operator's explicit, informed, ongoing, and freely revocable consent. The operator is the sovereign of their technology. This is not a configuration option. It is the foundational design requirement of all technology implementing this paradigm.

PRINCIPLE 2: IDENTITY IS LIVING

Human identity is not a credential. It is not a password, a fingerprint impression, a face photograph, a recorded voice, or any other static artifact that can exist independently of the person. Human identity, properly understood, is the living, continuously-changing physiological reality of a specific person alive at a specific moment. Any authentication system defeatable by capturing and replaying a static credential has not authenticated a person — it has authenticated a recording. Authentication must require the living person. Not evidence of them.

PRINCIPLE 3: DATA IMPERMANENCE

Human beings do not leave data trails in the physical world. When a person leaves a room, their words do not remain recorded on the walls. Technology must mirror this natural reality. Operator data exists only during authenticated sessions and disappears completely and irrecoverably when sessions end. This is not privacy by policy. It is privacy by architecture. No policy can be overridden by legal process. Architecture that makes data technically impossible to retain cannot be compelled to produce what does not exist.

PRINCIPLE 4: THE SOVEREIGNTY OF DESTRUCTION

Every human being has the absolute, unconditional, and non-delegable right to destroy their own data rather than surrender it to any party. This right is prior to and superior to any legal, governmental, regulatory, or commercial claim on that data. It is the digital form of the right against self-incrimination — the fundamental human right not to be compelled to provide evidence against oneself. This right does not permit obstruction of justice in response to valid lawful process. It does permit — and the present invention specifically enables — the exercise of this right before any legal obligation to preserve data has been established.

PRINCIPLE 5: SUCCESSION WITHOUT EXPOSURE

The death or incapacitation of a human operator must never create a security vulnerability. Operational authority transfers cryptographically to designated successors upon operator death or incapacitation without exposing the predecessor's credentials to any non-successor party, including adversaries who may physically possess the predecessor's equipment. In military contexts, this means continuous operational capability with zero intelligence value to any adversary who captures equipment. In civilian contexts, this means seamless inheritance without probate exposure.

PRINCIPLE 6: INDIVIDUAL CONSCIENCE IS INVIOLABLE

No technology implementation shall prevent any individual from exercising their conscience. In military and law enforcement contexts specifically: every individual operator retains the absolute and irrevocable right to destroy their own credentials and render their equipment inoperable rather than execute orders they believe to be unlawful, in violation of international humanitarian law, or contrary to fundamental human rights.

This is not insubordination. It is the practical implementation of Nuremberg Principle IV, which holds that individuals bear personal responsibility for crimes committed under orders. If technology makes it impossible to refuse by making compliance technically effortless, technology has removed the capacity for moral agency. Technology must preserve the individual's capacity to refuse.

PRINCIPLE 7: THE SECOND AMENDMENT TECHNOLOGY PRINCIPLE

The Second Amendment to the United States Constitution recognizes the individual right to keep and bear arms as the ultimate check against governmental tyranny. Technology applied to weapons must never diminish this right. No implementation shall enable any government or other party to remotely disable, restrict, or render inoperable any privately-owned weapon. All civilian weapon implementations must include an unconditional mechanical override returning the weapon to fully mechanical operation, operable by the owner without tools, codes, or external assistance, that cannot be remotely re-engaged by any party. The electronic capability is an addition. The mechanical function is the right. The right cannot be made contingent on the addition.

PRINCIPLE 8: VOTER PRIVACY IS ABSOLUTE AND ARCHITECTURAL

The secret ballot is the foundational guarantee of free elections. No implementation of operator-bound technology in any electoral system shall create, store, or permit access to any record connecting voter identity to ballot content, at any time, by any party, including by court order. This protection is achieved architecturally through one-way cryptographic commitment schemes, not by policy. Policy can be overridden. Mathematics cannot. All biometric data used for voter verification is destroyed immediately upon verification completion. Coercion resistance is provided by replacement ballot capability. No voter shall be able to prove to any third party how they voted, eliminating the technical basis for vote buying and voter coercion.

PRINCIPLE 9: ANTI-TYRANNY BY DESIGN

Every capability of operator-bound technology is a double-edged instrument. Authentication can verify identity or surveil it. Access control can protect or restrict. Destruction can defend data or be used offensively. The Anti-Tyranny Design Imperative requires that all implementations be designed so that the individual operator — not any government, corporation, or other entity — is the sole controller of all capabilities. Technology must not give any external party the ability to activate, restrict, monitor, or disable the operator's systems without the operator's explicit real-time consent.

PRINCIPLE 10: UNIVERSAL DATA IMPERMANENCE

The session-based data architecture applies universally to all host systems. No vehicle, hotel, rental service, terminal, medical facility, electoral system, financial institution, or other system implementing the operator-bound protocol retains any operator data following session termination. This universal impermanence eliminates the aggregate surveillance infrastructure that makes data collection across systems and sessions the foundation of modern control. If each system retains nothing, the foundation disappears.

PRINCIPLE 11: CHILDREN AND VULNERABLE PERSONS: PROTECTION NOT SURVEILLANCE

Protective monitoring of children and vulnerable persons is expressly designed for their benefit and operates exclusively under guardian control, for exclusively protective purposes, with no data accessible to any government without specific court order, automatic termination at legal majority, and full data control transferred to the formerly protected person upon majority. Protection must never become surveillance. Guardianship must never become control.

PRINCIPLE 12: THE FUTURE TECHNOLOGY COVENANT

These principles apply to all technology, present and future, regardless of implementation, form factor, operating medium, or application domain. Neural interfaces and brain-computer communication systems. Implanted biological sensors. Quantum computing systems. Biological computing. Synthetic biological systems. Any technology not yet conceived that authenticates human identity or controls access to systems. Technology changes. The human beings who use it do not. The covenant is permanent.

PRINCIPLE 13: OPERATOR SOVEREIGNTY IS ABSOLUTE

The authenticated human operator is, in all circumstances, under all conditions, and without any exception, the supreme authority over all data, systems, credentials, and technology bound to their identity. This authority is not granted by any government, licensed by any corporation, or contingent on any legal proceeding. It is inherent in the human being themselves. No court order compels a person to provide their heartbeat. No warrant seizes a person's neural patterns. The human body is the last inviolable private space. Technology built on physiological authentication inherits that inviolability.

PART III: ABSOLUTE PROHIBITIONS — PRIOR ART ON TYRANNICAL USES

The following uses are hereby placed in the public domain as prior art. No patent application may claim exclusive rights to these uses, as they are anticipated by this publication. Any commercial implementation of these uses as applied to operator-bound technology faces patent invalidity of any subsequently-filed patent, public domain dedication of the concept, and the licensing prohibitions of the accompanying patent application.

What This Technology Is Explicitly NOT For

- ✗ Mass surveillance of any population without specific individual consent
- ✗ Remote disabling of any privately-owned weapon by any government or party
- ✗ Social credit scoring, behavioral rating, or trustworthiness scoring of any person
- ✗ Restriction of movement based on technology-collected data without judicial process
- ✗ Restriction of financial access as behavioral control or punishment
- ✗ Mandatory biometric enrollment without full and free informed consent
- ✗ Government backdoors, master keys, or override capabilities of any kind
- ✗ Remote monitoring of location, activity, or associations without explicit consent
- ✗ Posthumous account access without explicit advance authorization by the deceased
- ✗ Identification of non-voting eligible voters or tracking of voting participation
- ✗ Any connection between voter identity and ballot content under any circumstances
- ✗ Use of electoral systems by any political party, campaign, or political organization
- ✗ Voter suppression through technical authentication failures of any kind
- ✗ Behavioral modification through technology of any kind
- ✗ Elimination of mechanical override in any civilian weapon implementation
- ✗ Network dependency for any privately-owned weapon's operability
- ✗ Simultaneous remote disabling of multiple privately-owned weapons
- ✗ Preventing soldiers from disabling their own credentials to refuse illegal orders
- ✗ Child surveillance beyond protective guardian monitoring with automatic termination
- ✗ Tracking of religious practice, political belief, or personal association
- ✗ Discrimination based on biometric characteristics or authentication history
- ✗ Any use a reasonable person would recognize as contrary to human dignity and freedom

What This Technology IS For

- ✓ Protecting individual data from seizure, surveillance, and unauthorized access
- ✓ Enabling individuals to destroy their own data rather than surrender it
- ✓ Binding technology to serve its operator rather than any possessor
- ✓ Preventing weapons and vehicles from being used against their owners
- ✓ Protecting children from abduction and trafficking through guardian-controlled monitoring

- ✓ Enabling military operators to protect classified information from capture
- ✓ Providing journalists with reliable data protection against seizure
- ✓ Enabling the practical exercise of the right against self-incrimination
- ✓ Secure succession of lawful operational authority without credential exposure
- ✓ Protecting individual conscience in all employment and command contexts
- ✓ Preserving the balance between armed citizens and their government
- ✓ Enabling free, secret, verifiable, coercion-resistant elections
- ✓ Protecting electoral integrity without creating voter surveillance infrastructure
- ✓ Providing universal access to identity and authentication without government dependency
- ✓ Preventing identity theft, financial fraud, and impersonation of any kind
- ✓ Giving every person on earth practical sovereignty over their digital identity

PART IV: PRIOR ART — APPLICATION CONCEPTS IN PUBLIC DOMAIN

The following application concepts are placed in the public domain. The general concept of each application is prior art. The specific technical implementations described in the accompanying patent remain protected. Any party may implement the general concept. No party may implement the specific patented methods without a license compliant with the Human Sovereignty licensing conditions.

DOMAIN	CONCEPT IN PUBLIC DOMAIN
Portable Data Security	Person-carried device providing emergency liveness-verified destruction of digital storage media, rendering data forensically irrecoverable without network connectivity.
Integrated Storage-Auth-Destruct	Single device combining hardware security key authentication, encrypted data storage, and self-destruction capability, with no data recoverable following destruction.
Smartphone Platform	Smartphone integrating all personal security platform capabilities including data destruction, credential management, and dead man's switch, serving as computing root of trust.
No-Storage Computing Terminal	Computing terminal containing no internal storage, booting exclusively from authenticated portable operator device, leaving no data on terminal at session end.
Vehicle Authentication	Vehicle operable exclusively by authenticated operator, storing all settings in volatile memory, purging all data at session end, supporting temporary permission delegation.
Military Succession	Military equipment authentication with chain-of-command succession destroying predecessor credentials on operator death, preventing adversarial intelligence value.
Access Control — Universal	Building, hotel, transit, and property access systems storing no access history, accepting only authenticated operator credentials, supporting time-limited delegation.
Voter Verification	Electoral authentication architecturally incapable of connecting voter identity to ballot content, with immediate biometric destruction and coercion resistance through replacement ballot.
Electoral Integrity	Verifiable election integrity through aggregate cryptographic proofs without any individual voter identification, participation tracking, or ballot attribution.
Financial Authentication	Liveness-verified payment and banking requiring living operator presence, preventing posthumous access and detecting coerced transactions.
Border Crossing Identity	Digital travel identity using living biometric, storing no crossing history in border systems, permitting credential destruction at operator's choice.
Medical Records	Patient-controlled medical records stored on patient device, accessible

	only to specifically authorized providers for specific purposes, purged after use.
Child Protection	Guardian-authenticated child monitoring detecting unauthorized separation, operating exclusively under guardian control, terminating at legal majority.
Elder Care Protection	Protective monitoring of persons with cognitive impairment, exclusively guardian-controlled, strictly limited to safety purposes, creating no surveillance infrastructure.
Smart Home and IoT	Home and IoT systems operable exclusively by authenticated operator, storing no operator data in home systems, purging all data at session end.
Ownership Verification	Cryptographic ownership proof for any property, transferable only by authenticated owner, destroyable to prevent adversarial exploitation.
Wearable Liveness Monitoring	Wearable device of any form factor providing continuous cardiac and physiological monitoring, relaying liveness status to connected operator devices.
Implant Integration	Implanted device providing continuous biometric authentication and physiological monitoring, triggering dead man's switch protocols upon vital sign cessation.
Neural Interface Authentication	Brain-computer interface providing neural pattern authentication and continuous neural activity monitoring for liveness verification and dead man's switch.
AR / Smart Glasses	Head-mounted display providing ocular biometric authentication, threat awareness overlay, and hands-free covert destruction triggers.
Smart Ring	Ring-form wearable providing continuous cardiac monitoring and NFC authentication, dead man's switch relay, and covert gesture triggers.
Remote Networked Destruction	Authenticated remote destruction commands via any communication means coordinating simultaneous destruction across multiple registered devices.
Satellite-Triggered Destruction	Destruction command delivery via satellite independent of terrestrial network infrastructure, enabling remote destruction in any geographic location.
Civilian Weapon Authentication	Weapon operable exclusively by authenticated owner with unconditional mechanical override, no remote disable capability, and no network dependency.
Voting Rights Preservation	All electoral implementations preserving secret ballot, coercion resistance, no voter surveillance infrastructure, and architectural impossibility of ballot attribution.

PART V: CONSTITUTIONAL AND HUMAN RIGHTS FRAMEWORK

Every principle and prohibition in this document is grounded in recognized constitutional and international human rights law. This section establishes the legal basis confirming that these principles are not novel restrictions — they are existing rights receiving technical implementation for the first time.

United States Constitutional Framework

First Amendment: No implementation shall surveil, track, record, or restrict any person's speech, press activities, religious practice, political associations, or assembly.

Second Amendment: No implementation shall enable remote disabling of privately-owned weapons. Mechanical override is mandatory in all civilian weapon implementations. No network dependency for weapon operability. No simultaneous mass disable capability.

Fourth Amendment: The right to destroy one's own data is the digital exercise of the right against unreasonable search and seizure. No implementation shall prevent exercise of this right prior to service of valid legal process.

Fifth Amendment: No implementation shall compel biometric authentication against an operator's will. The right against self-incrimination applies to all authentication. Forced authentication is compelled self-incrimination.

Ninth Amendment: The right to digital privacy and data sovereignty is a fundamental unenumerated right. The rights protected by this paradigm are not limited to enumerated constitutional rights.

Fourteenth Amendment: No implementation shall enable discrimination on any protected basis or deny equal access to the platform's protective capabilities.

International Human Rights Framework

UDHR Article 3: Right to life, liberty, and security — implemented by preventing technology from being turned against operators.

UDHR Article 12: Right to privacy — implemented architecturally through data impermanence and operator-bound access.

UDHR Article 13: Freedom of movement — no implementation restricts movement based on technology data without judicial process.

UDHR Article 17: Right to own property — digital property and credentials are exclusively owned by the operator.

UDHR Article 19: Freedom of expression — no surveillance of communications through any implementation.

UDHR Article 20: Freedom of association — no monitoring of associations or memberships.

UDHR Article 21(3): Secret ballot — voter verification implementations are architecturally incapable of ballot attribution to voter identity.

ICCPR Article 17: Binding treaty privacy right — all state implementations in 173 signatory states must comply.

ICCPR Article 25: Right to vote by secret ballot — implemented architecturally not merely by policy.

ECHR Article 8: Right to private life — all implementations in Council of Europe member states must comply.

Geneva Conventions: All military implementations comply with laws of armed conflict. Nuremberg Principle IV implemented through individual conscience protection.

CRC Articles 16, 19, 35: Child privacy, protection from violence, and anti-trafficking — all child protection implementations designed to implement these rights.

Convention Against Torture: No implementation enables torture, coercive interrogation, or use of physiological monitoring for coercive purposes.

UN Guiding Principles (Ruggie): All commercial licensees accept Principles 11-21 corporate human rights responsibilities.

PART VI: LEGAL NOTICES, DEDICATION, AND ANTI-SUPPRESSION MEASURES

CC0 Public Domain Dedication

The principles described in Part II, the prohibitions described in Part III, and the application concepts described in Part IV are hereby irrevocably dedicated to the public domain under Creative Commons CC0 1.0 Universal Public Domain Dedication. To the maximum extent permitted by law, the author waives all copyright and related rights in these principles, prohibitions, and concepts. They may be used without permission, attribution, or restriction.

Prior Art Declaration

This document constitutes prior art under 35 U.S.C. § 102 and equivalent provisions in all jurisdictions as of its publication date. Any patent application filed after this date seeking to claim exclusive rights to any principle, prohibition, application concept, or combination described herein is anticipated or rendered obvious by this publication and is subject to rejection or invalidation on that basis.

The following specific concepts are placed in the public domain as prior art: operator-bound technology in any form; physiological liveness authentication as a data destruction trigger; dead man's switch data protection in any portable or wearable device; selective destruction of individual device components or data containers; universal data impermanence across host systems; military operational succession without credential exposure; individual conscience protection through self-destruction capability; child protection through guardian-authenticated monitoring with majority termination; voter verification architecturally incapable of ballot attribution; civilian weapon authentication with mandatory mechanical override and no remote disable; and all other concepts described in Parts I through V.

Anti-Suppression Architecture

This document has been simultaneously submitted for permanent archiving to: Zenodo.org (CERN — permanent DOI, primary archive); Internet Archive — archive.org/upload; arXiv.org preprint server (cs.CR category); Electronic Frontier Foundation — info@eff.org and press@eff.org; Committee to Protect Journalists — info@cpj.org; Reporters Without Borders US Desk — dcdesk@rsf.org; Freedom of the Press Foundation — info@freedom.press and press@freedom.press; American Civil Liberties Union — aclu.org/contact-us; and legal counsel holding notarized copies in escrow in at least three different national jurisdictions.

Any attempt by any government, agency, court, or other authority to classify, seal, restrict, or suppress this document after the date of initial publication: (1) is legally ineffective as to published prior art which cannot be retroactively classified; (2) will be publicly disclosed by the archiving organizations listed above pursuant to their stated missions; (3) will itself become public information through the multi-jurisdictional escrow arrangement; and (4) constitutes evidence of the precise tyrannical impulse this document was designed to prevent and document.

Notice to All Governments

These principles do not prevent legitimate law enforcement, national security operations conducted within the rule of law, or enforcement of valid judicial process. What they prevent is the use of this technology as an instrument of mass surveillance, arbitrary control, or extrajudicial restriction of any human being without specific individual legal process and judicial oversight. Governments that implement these principles faithfully will find them entirely compatible with lawful governance. Governments that cannot implement these principles compatibly with their governance practices have revealed something important about those governance practices.

Notice Regarding the Second Amendment

The Second Amendment provisions in this document and the accompanying patent reflect a specific and serious concern: that authentication technology applied to weapons could be used to nullify the Second Amendment without constitutional process by making civilian weapons dependent on government-controlled authentication infrastructure. The mechanical override mandate and the prohibition on remote disable are not safety concerns — they are freedom concerns. A weapon that functions only when a government server authorizes it is not a privately-owned weapon in any constitutionally meaningful sense. This technology will never be licensed for that purpose.

Notice Regarding Voter Privacy

The voter privacy provisions reflect the conviction that the secret ballot is the single most important protection for democratic participation. Vote buying, voter coercion, and voter suppression all depend on the ability to connect specific voters to specific ballots. The architectural impossibility of that connection — achieved through one-way cryptographic commitment rather than policy — eliminates the technical basis for all three. No court order, no government mandate, no emergency, and no commercial arrangement will ever produce a licensed implementation capable of connecting voter identity to ballot content. This is not a policy commitment. It is a mathematical one.

A Note to Future Inventors and Implementers

Build on this. Extend it. Find applications we have not imagined. The public domain dedication ensures you need no license from us to implement these principles. The only thing we ask — not require, but ask — is that you implement them faithfully: technology serves the operator, data is impermanent, destruction is the operator's right, conscience is inviolable, the ballot is secret, the weapon is the owner's, and no technology is ever turned against the person it was designed to serve.

That is the whole of it. Everything else is implementation.

CONCLUSION: THE WORLD THIS MAKES POSSIBLE

The Human Sovereignty Technology Paradigm describes a world that is technically achievable with current and emerging technology. A world where data theft is impossible because data does not persist. Where identity theft is impossible because identity requires a living body. Where surveillance requires the individual's ongoing consent. Where weapons cannot be turned against their owners. Where the ballot is mathematically secret. Where every soldier can refuse an illegal order. Where every child is protected without being tracked. Where every person on earth has the same practical sovereignty over their digital identity regardless of wealth, citizenship, or technical sophistication.

This world is not built by any single device or any single inventor. It is built by establishing principles that orient all technology toward human freedom and enshrining those principles in the permanent public record before any government can prevent it. We have done our part. The principles are published. The prior art is established. The tyrannical uses are in the public domain. The protective uses are in the patent. The rest is implementation.

> *The measure of any technology is not what it can do. It is who it serves. We have built something that serves only the living person who uses it, and we have published these words to ensure it can never be otherwise. This is our commitment to every person who will ever use this technology, and to every person who never will.*

Published: March 29, 2026

Filed simultaneously with: US Provisional Patent Application

Archived: Zenodo.org (DOI) | archive.org | arXiv.org | info@eff.org | info@cpj.org | info@freedom.press | dcdesk@rsf.org | aclu.org/contact-us

License: CC0 1.0 Universal — Irrevocably in the Public Domain

Cannot be classified. Cannot be suppressed. Cannot be unwritten.

[END — THE HUMAN SOVEREIGNTY TECHNOLOGY PARADIGM — VERSION 2.0 FINAL]